Emergent Issues of Network Centric Architectures and Shared Infrastructures

Marie V. Stella, CISSP
mvstella_99@yahoo.com
202 685-3046

System Engineering (SE)and Information Technology (IT)

Relatively new disciplines

Based on Rational Thinking Models of 1900”s

Unexpected growth in IT with increased need for SE

IT based systems are growing in complexity and unpredictability

SE based on assumption of “ordered” world

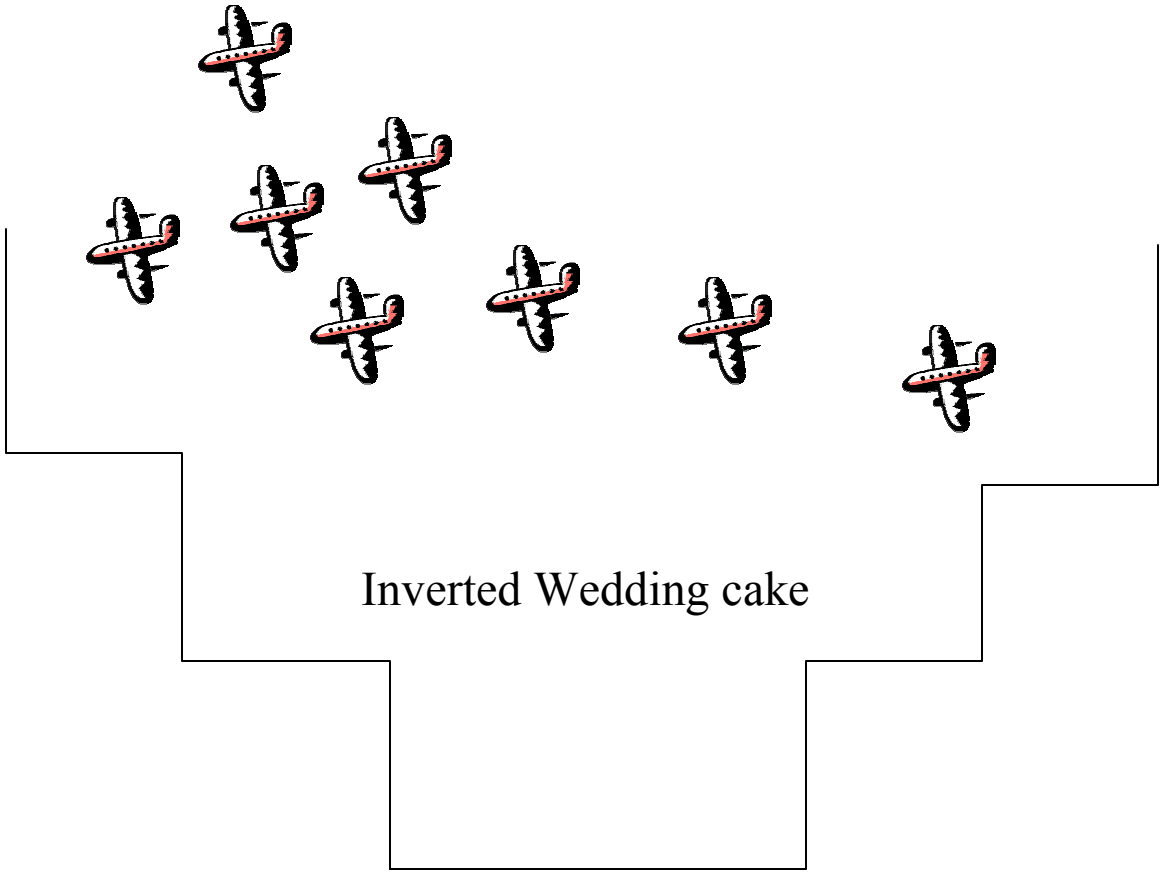
Proposal: Revolutionize SE Thinking

The Cartesian Method

- Accept nothing as true which is not clear and distinct;
- Analyze a problem into its parts and discuss it part by part;
- Arrange thoughts from simple to complex as the order of study;
- Enumerations must be full and complete and nothing must be omitted.

What does this mean?

Average Joe/Jane



Inverted Wedding cake

System Engineer Joe/Jane

NAS Modernization,

why isn't it working?

Underway for over 25 Years

- Perform acceptable SE processes
- Address interfaces
- Formalize Program Risk Analysis
- Formalize security Risk Analysis
- Utilize management processes like CMM, IPTs, CC*, Spiral Development*
- Predictive Modeling Techniques and cost/benefit analysis

We treat the NAS like a machine and minister to its parts

CMM – Capability Maturity Model, IPT – Integrated Product Teams, CC- Common Criteria,

Complexity and the NAS

The Modern National Air Space (NAS)

- Sub-networks composed of secure military, civilian national NAS operations and a shared NAS with International and business partners,
- Vehicle diversity that includes sub-sonar, sonar and unmanned aerial vehicles sharing the same and, for the most part, unrestricted airspace,
- Traffic Pattern and Separation changes that are driven by new technology and requirements for increased air space flexibility,
- Work load and work description changes driven by new technology and outsourcing and privatization of functions such as telecommunications.

NAS Sub-Networks

- Shared infrastructures (military/civilian/private) each designed to meet different needs, threats, partnerships and workspace requirements,
- Increased and changing threats to civil infrastructures and possible increases in vulnerabilities of commercially available system introduced by the military and homeland defense use of civilian infrastructure,
- Increased and changing threats to military and homeland defense networks by incorporating COTS equipment and untrusted civilian and private partners/networks into the information chain and infrastructure,
- Increased costs to government, and possibly, to the private sector to operate, maintain and harden shared systems,
- Multiple operations and monitoring and maintenance systems with different goals, systems and skills levels,
- Increased and multiple sources of information that must be blended and secured.

Vehicle diversity

•Sub-sonar, sonar and unmanned aerial vehicles sharing the same, unrestricted airspace:

UAVs – Predator in super high airspace, cargo, drug and border crossing detection, etc., etc. etc.

Military Jets – continued and increased

General Aviation – increased

Regional Aircraft – increased

On Board Security Countermeasures effecting plane and airspace

•Increased pilot and controller workload

(delay of new technologies – schedule, funding, acquisition problems) that may support diversity)

Traffic Pattern and Separation changes

September 11th fact - grounded airway is not only bad for the airlines but for the American economy and homeland Defense –

Need a new Airspace Topology

- •Rapid Transformation of Airspace
  - -Continuation of Service,
  - -Accommodate changing flight patterns, demands and unpredictability resulting for terrorism, rapidly changing defense and civilian needs,
- •Holistic Approach that addresses civilian, government, industry collaboration, airline collaboration, multi-modal approach to transportation,
- •Collecting, sharing and manipulation of data securely without violating privacy, Competition and ownership laws,

Protection of data and the ability for industry to move from competitive mode to partnerships and back again will be a major challenge and effect business strategies

Work load and Work Description Changes

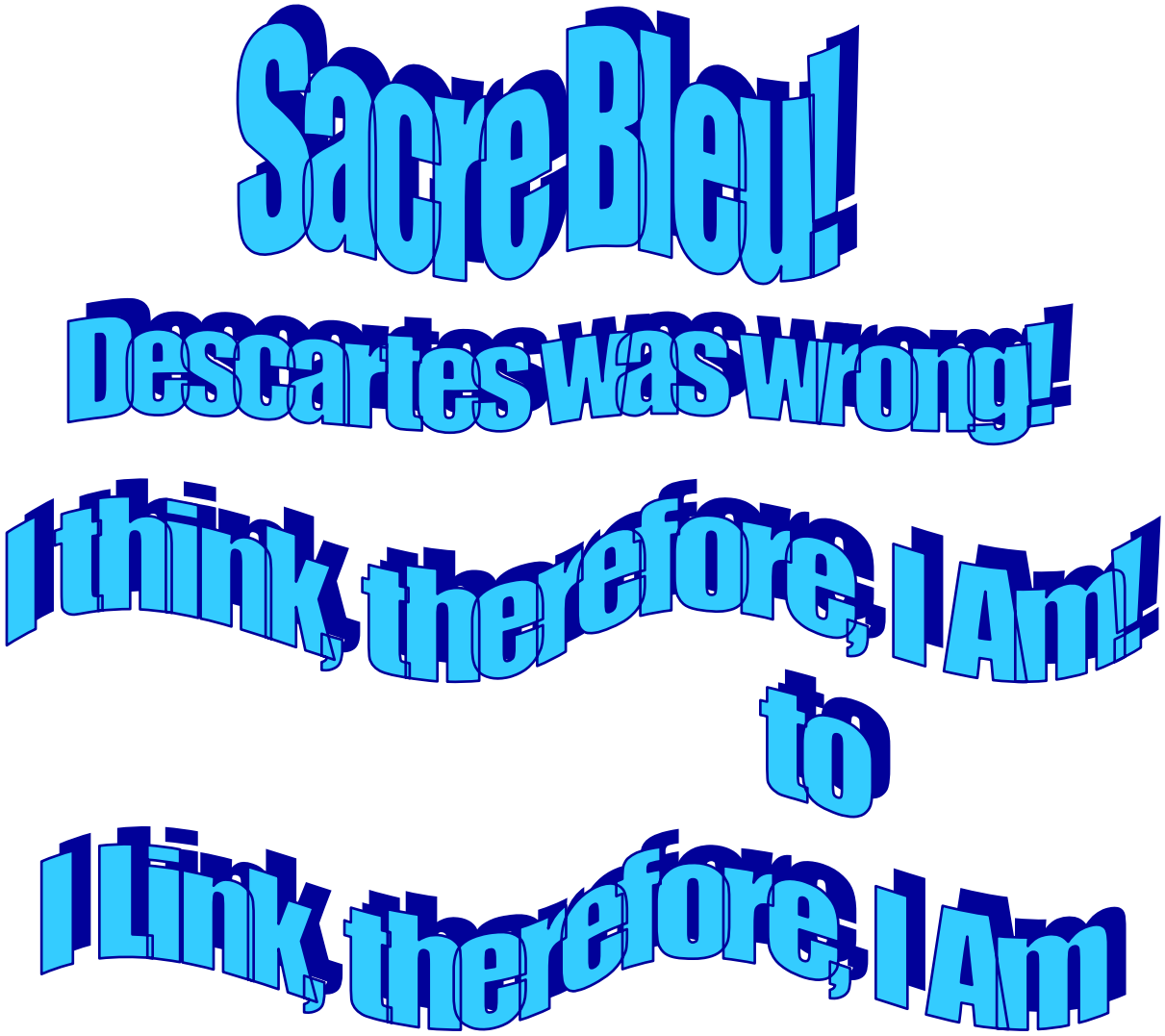
Machine-based NAS – homogenous, proprietary, de facto government standards, ruggedized, reliable, available, and system integrator managed components.

•**Network Centric Based NAS** - Scalable networks, Internet/IP private and public networks lack robustness and known weakness and vulnerabilities- increase with ubiquitous use. (IP may not meet performance and reliability of future networks and European and Asian developed open system protocols and systems may overtake this technology.)

•Interconnected to various partners with different level of trust - weakens entire chain of communications, increase complexity of system monitoring, fault detection, correction, restoral and forensics

•Mandated COTS systems not associated with safety and high performance systems, ubiquitous use has cascading effects when deliberately or accidentally compromised. No access to source and application code, no insight into code aberrations or the ability to develop quick fixes to operational systems with software glitches that effect safety.

•Outsourcing NAS networks through programs or subcontracting to both American and foreign entities leaving NAS systems vulnerable to end-source attacks and loss of situational awareness Outsourcing will leave a weakened FAA maintenance workforce and dissuade recruitment of quality technicians willing to commit to *manage and maintain legacy systems.*



The hard problems-building flexible NAS in an era of terrorism, growing global market with increased third world competition, and, perhaps a weakened economy

New Thinking about NAS SE

As we move from machine to network-centric based IT we must build to loosely understood emergent behaviors of both people and systems. This requires;

- Greater up-front understanding of enterprise and program objectives and behaviors,
- Use of flexible risk processes that may be, in part, effects based,
- Ability to influence rapid changes to national and international policy,
- Change in organizational procedures and structure that compliment network centric information design,
- Improved modeling and validation of operational and system concepts at the inception of programs.

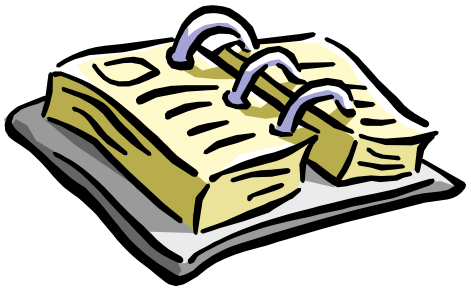
Building a new NAS SE Process
Suggestions

SE egotism: All systems begin, operate and die based on the constraints of the SE process.

This is not enough!

SE must be driven by an overarching

Transportation Plan and Policy



Transportation Plan and Policy

Goals must be clearly articulated and demonstrate real progress

Multi-disciplinary and multi-agency/industry effort

Planning requires skills of:

- Economists and international strategist and policy makers,
- Legal experts, who understand the NAS but also civil liberties, national and international competition and laws, national budgets and tax structures, export and tariff regulation,
- Members who understand military and policing actions to address security detection, intervention and forensics in globally interconnected world,
- Risk Managers who are true risk statisticians

Transportation Plan and Policy

Policy must take into account:

International standards and rulemaking constraints and must be designed to facilitate timely universal agreements on interoperability and standards,

Policy must be freed of pre-supposed solutions to poorly defined issues and encourage innovation,

Metrics must be developed that ensure policy and activities meet national objectives,

Models that address uncertainty from a political, behavioral, economic and technical uncertainty must be developed to help policy makers understand risks of decisions made.

NAS Concept of Operations and Associated Contingency Plan

CONOPS and Contingency plan must focus on flexibility, contingency and home land defense

Modeled and evaluated under various scenarios during their development to understand impact of unexpected events and how element failures will effect robustness of NAS,

Must include roles, responsibility and communication process for other transportation modalities, military, private industry and international entities.

Real Reform of the Acquisition and Budget Process

NAS new acquisitions are dominated by a few corporations and technology that is 10 and sometimes 20 years old. The FAA pays to upgrade no longer supported equipment prior to it even being installed.

The NAS requires:

Early adaptation of innovation,

Less expensive entry for small business and new companies,

Ability to make frequent and early corrections to problems as they are identified

This requires a more proactive approach to managing acquisitions and a radical change in the way we write specifications and manage contracts.

This a new art and may require analysis and research to understand how successful innovation is captured and implemented in industry and abroad.

Reform of the Acquisition and Budget Process

New systems requirements must be married to a top-down FAA enterprise-wide requirements and design:

The system improve overall operational concept,

Must include early testing of concept, possibly through modeling and simulation, to demonstrate how new requirements and associated benefits effect the NAS,

Improved and early international and national agreements and certifications,

Early analysis of how new system fits into the NAS chain of communication regardless of level of system (critical, essential, routine) to identify early risk or changes in security operations, etc.

Reform of the Acquisition and Budget Process

The new NAS SE security plan must be:

Flexible and robust enough to change topologies under attack.

Securely) identify “critical components” that must remain viable to allow safe flight under attack - requires input from operation personnel and industry and international community.

Include technically strategies to harden, gracefully degrade or self-heal vital network components, and allow others to fail securely.

Shift from component to enterprise security planning. And be able to detect, isolate, heal, and perform forensics on operational NAS networks without effecting performance.

Support research and collaboration.

Reform of the Acquisition and Budget Process

The specification process had evolved from detailed designs based on government developed prototypes to high-level performance specs. Many specs actually allow contractors to develop requirements especially in the area of security, after contract award. Small companies, who provide new technologies, are dissuaded from subcontracting because of high overhead, long schedule slips and associated payment delays.

The Acquisition metrics must change to encourage early, open dialogue regarding program issues and reduce punitive behaviors towards employees and contractors. Metrics should be program specific and measure critical program challenges and not general acquisition processes.

Prototype Development and Testing

Do the hard things first and make sure the concept works!!!!! Prototyping must address technical and operational challenges.

Identify challenges through a vigorous risk assessment process.

Testing should begin early and include agent based/effects based scenario modeling and gaming techniques that simulate operational concepts.

Earlier and more cost effective methods must be developed. Testing required greater collaboration and test procedures must be written to ensure independence of oversight testing.

Risk Assessment and Metric Development

Risk Assessment and Metric development must become dominant disciplines in agency!

Focus must shift from due diligence in successfully implementing process to successful program implementation.

The government needs a new risk paradigm and must recruit and train professional risk statisticians.

Life Cycle Analysis and Maintenance Strategies

Maintenance strategies must assure continuous operation, safety and security.

NAS must be designed for robustness and prevention, rapid detection, and restoral of services under attack or accidental disruption,

Strategies to accomplish this must include:

- Access and ability to change code and reconfigure systems,
- The ability to work jointly with managers and administers of DOD/civilian agencies, national and international partners to implement strategies, restore networks and perform forensics and take legal action,
- Revisit OMB A-76-if only legacy systems remain in the NAS, retaining and recruiting technicians will not be effective.

Strategies to maintain the NAS must be prominent in NAS Policy, Concept and Contingency Plans and System Requirements

Research and Education

No current research and funding model:

- Government no longer funding research efforts
- Industry research (and rebuilding of aging infrastructure) is limited,
- Companies are spending research money abroad,

Engineering and scientific education and training must be revitalized to include:

- Network Centric and emergent technologies and behaviors,
- Incentives to better prepare and encourage students to engage in technological studies must be encouraged.

INCENTIVES for research, modernizing the infrastructure, and education must be adopted by Government.

New Leadership Skill Sets

New skills must include:

Focus on Risk Reduction and flexible strategies,

Focus on how information will be used, moved, and by who,

Understanding of how organizational cultures effect implementation,

Improved strategic thinking and long term planning skills so that commitment to standards, international agreements and critical senior level functions can be recommended and trusted to be implemented.

The Way Ahead

Today we have plans and procedures for all the items discussed. They don't work effectively in a machine-based mind set. The NAS must be considered a dynamic, complex system for it to be properly understood.

Combining the current domain knowledge with new modeling techniques and a better understanding of complexity is needed to take an innovative approach to designing a new NAS.

Strategic thinking and planning must be in place to harness the changes we are facing today in the economy, home land defense and competitive marketplace.